Assessment of Software Development Tools for Safety Critical Real-Time Systems

Dr. Andrew J. Kornecki, Dr. Nick Brixius
Department of Computing, Embry-Riddle Aeronautical University, Daytona Beach, FL 67260

The main objective of this research project is to identify the assessment criteria that allow both developers and certifying authorities to evaluate specific safety critical real-time software development tools from the system/software safety perspective. Related objectives are to present and evaluate the state of art in safety critical software development tools and generate a set of guidelines for tool selection. The intended audience for the research outcome includes program/procurement managers, project leaders, and system/software engineers directly involved in implementing real-time safety critical systems.

The research team members include faculty of the Department of Computing and graduate students from the Master of Software Engineering program at Embry-Riddle Aeronautical University.

Safety critical real-time systems continue to become more complex. They often operate in uncertain environments and must provide reliability, fault tolerance and deterministic timing guarantees. The software for such systems is developed using a variety of tools that must address these issues. Appropriate tool must be selected to meet the needs of a specific project.

Software engineering tools, often termed as Computer Aided Software Engineering (CASE), assist in the development of software intensive systems. A tool is defined as a computer program used to help develop, test, analyze, or maintain another computer program or its documentation. The current state of art includes a variety of tools, which often support more than one phase of the software development lifecycle.

There are not many comprehensive efforts on tools evaluation and assessment other than an occasional paper at technical conferences reporting on experience with one or the other tool. Exceptions are the IEEE standards documents on the topic, describing the recommended practice for adoption and guidelines for CASE tools selection, and RTCA Document DO178B that addresses software considerations in airborne systems and equipment certification. Also the Software Engineering Institute (SEI) published a technical report that provides a good starting point for tool assessment, proposing tool taxonomy and an evaluation framework.

Desired characteristics of modern tools include multi-user development, shared information repository, integration with external tools and applications, requirements modeling, executable specifications, use of established software engineering notations, reliable code generation, performance analysis, verification and validation of the system. The issue is whether a specific tool is really facilitating the product development for an experienced developer or only hand-holding an inexperienced user. In either case, the resulting target code depends heavily of usability, correctness, and precision of the tools used for the code creation. If properly designed and used, software tools may eliminate or reduce the human errors that are often introduced in

software life-cycle. On the contrary, a marginal and/or improperly used tool may result in faulty end-product with potential significant impact on target system reliability and safety.

The project was proposed as three-phase activity, as described briefly below. The first phase is currently supported by FAA Contract DTFA03-01-C-00048. Propagating project results shall be accomplished by briefings for the governmental agencies and interested industry contractors, and by publishing research materials on the Internet.

The first phase of the project (January 7, 2002 – January 6, 2003) includes:

- A thorough review of the existing tools used for real-time safety critical software development.
    - Identify the existing and available tools researching the vendor offerings, journals, conference proceedings, web sites, and using industry contacts
    - Identify the general categories of tools used for the real-time development.
    - Selection of the relevant tools based on their perceived merit and the industry feedback
- Research and define the tool assessment criteria based on the established software/system safety standards, processes and procedures, with particular references to DO178B.
- Creation of a taxonomy and set of criteria for the tool selection by modifying and adapting the SEI taxonomy for use with real-time safety critical products.
    - The approach shall be to find the relation between the identified characteristic features of real-time safety critical systems and the properties of the tools.
    - The real-time system characteristics include timeliness, responsiveness, schedulability, predictability, safety, reliability.
    - Typical examples of the tool properties will be their conformance to standards, modularity and scalability, speed and efficiency, support conceptual redundant design models, appropriate diagramming notations, traceability, consistency, vendor reputability, cost and availability, user community, etc.
- Identify set of tool selection criteria and create an appropriate questionnaire to be used for an industry survey.

The work in this phase shall be completed with selection of candidate tools based on validated criteria and the tools initial evaluation with respect to the established criteria.

The second phase of the project addresses the tools selected for the detailed evaluation. Also, a typical small-scale real-time project will be chosen to be executed using the selected tool(s). The rationale is the need to collect practical tool(s) use data in experimental conditions to facilitate tool assessment and evaluation. This phase shall include execution of the selected project while collecting appropriate effort and defect development process data. The second phase also includes analysis of the industry/government feedback in order to modify and further define the tool evaluation criteria with more stress on the product safety.

The third phase of the project shall include the completion of the data collection from the project execution and the analysis of the collected data. The issues addressed in this phase include the definition of tool usage process and related team efficiency. Also, an attempt will be made to analyze the required personnel skills when using the tool. The third phase shall also include work on final report and the propagation of results.